17-187M

REDACTED

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT TO SEIZE PROPERTY

I, Scott McDerby, being first duly sworn, hereby depose and state as follows:

1. I am a law enforcement officer of the United States who is empowered by law to conduct investigations of and make arrests for offenses enumerated in Title 18 of the United States Code.

2. I am a Special Agent with the United States Secret Service ("USSS") assigned to the Wilmington, Delaware Resident Office since June 2009. As a Special Agent, I have been involved in numerous criminal investigations, including investigations involving Computer Fraud, Credit Card Fraud, Financial Institution Fraud, Wire Fraud, Identity Theft, and various other crimes in my more than 17 years as a USSS Special Agent.

3. I am presently involved in an investigation of various subjects in connection with a scheme to defraud in violation of Title 18, United States Code 1028 (Identity Theft); Title 18, United States Code 1029 (Access Device Fraud); Title 18, United States Code Section 1343 (Wire Fraud), Title 18; United States Code Section 1349 (Conspiracy to Commit Mail and Wire Fraud); and Title 18, United States Code Sections 1956 and 1957 (Money Laundering) (collectively, "Target Offenses"). I make this affidavit in support of an application for a seizure warrant to seize the contents of the Poloniex account of Grant West ("West"), which is believed to contain BTCs.

4. Based upon my training and experience, and the facts and circumstances set forth below, there is probable cause to believe that West, aided and abetted by others both known and unknown, organized, operated, and controlled "hacking" campaigns against both United States and international corporations. West used a software package that tests large data sets of user

names and passwords, and then sold the verified credentials on the dark web.

5. I further submit there is probable cause to seize all monies and other things of value, including the digital currency Bitcoin, contained in the Poloniex account of West ("THE SUBJECT ACCOUNT") pursuant to Title 18, United States Code, Sections 981, 982 and/or 984, on the grounds they constitute or are traceable to proceeds of violations of Title 18, United States Code, Sections 1028, 1343, and 1349, and/or property involved in violations of Title 18, United States Code, Sections 1956 and 1957. For reasons set forth below, probable cause exists to seize property for civil forfeiture pursuant to Title 18, United States Code, Section 981(b)(1) and for criminal forfeiture pursuant to Title 21, United States Code, Section 853(f), by Title 18, United States Code, Section 982(b)(1). The property is subject to civil forfeiture in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 981(a)(1)(A) and is subject to criminal forfeiture in accordance with Title 18, United States Code, Section 982(a)(1) and Title 18, United States Code, Section 981(a)(1)(C), by Title 28, United States Code, Section 2461(c).

6. The information provided in this affidavit is based upon my personal knowledge, observation, analysis of bank and public source records, and information provided by other law enforcement officers and investigators involved with me in the investigation described below. During this investigation, I have collaborated with the USSS's London Office and our Asset Forfeiture Branch, which has over five years' experience in seizures of digital currency and blockchain analytics. This affidavit is being submitted for the limited purpose of securing a seizure warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are essential to establish the necessary foundation for the requested seizure warrant.

THE SUBJECT OF THIS INVESTIGATION

7. West was born on [redacted]. He currently resides at [redacted] Minster on Sea, Sheerness, Kent, ME12 4JF, United Kingdom ("UK"). The residence is rented in his father's name. West has no recorded employment, and has paid no UK tax in the past three years.[1] Accordingly, your affiant is not aware of any legitimate income source for West, with the exception of more recent receipt of welfare benefits in the UK. Nonetheless, he maintains a lavish lifestyle with international travel, expensive cars, and high-tech electronic devices.

8. Based on information obtained by the UK Metropolitan Police Service ("MPS"), West is believed to have been a prolific "hacker" of personal financial information. It is believed he used a software package called Sentry MBA. This is a credential stuffing tool, whereby large data sets of usernames and passwords are tested against online vendors' logon pages.

9. West utilized Sentry MBA to validate the usernames and passwords of users of online vendors' websites, and then trafficked them on several dark web market sites.

10. The MPS arrested West on 12/8/15, and executed a search warrant on his residence. As explained further below, they obtained evidence that West owns a substantial amount of the digital currency Bitcoin (hereinafter referred to as "BTC").

11. Poloniex, a Delaware corporation, manages West's BTC accounts. Poloniex is a money services business which operates as a digital currency exchange. They offer a number of services, including cryptocurrency trading. They also provide web-based BTC wallets. Like a safety deposit box, they securely store and provide access to the wallet holder's BTC funds. The role of cryptocurrency exchangers and web-based wallets is explained below.

---

[1] In the UK, if an individual is employed, he/she is automatically enrolled into the UK tax scheme, whereby taxes are deducted from his/her pay.

BACKGROUND REGARDING BTC, BTC EXCHANGERS, AND WALLETS

12. Based on my experience in this investigation, I know the following about BTC. BTC are a form of digital or virtual currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a decentralized, "peer-to-peer" network.

13. To acquire BTCs in the first instance, a user typically must purchase them from a BTC "exchanger." In return for a commission, BTC exchangers accept payments of conventional currency, which they exchange for a corresponding number of BTCs based on a fluctuating exchange rate. An exchanger can be a money services business registered with the U.S. Department of the Treasury or simply a person in the community buying and selling BTC to others.

14. When a user acquires BTCs from an exchanger, the BTCs are sent to the user's BTC "address," analogous to a bank account number, which is designated by a complex string of letters and numbers. In order to receive the BTC and conduct transactions, the user needs a BTC "wallet." The wallet is the software that stores the user's BTC public addresses (or "public keys") and also the private encryption keys necessary to transfer the BTC in a transaction. Both the public address or key and the private key are necessary to conduct a BTC transaction. The public key is the account number and the private key is the secret key, like a password, that gives you the authorization to use the BTC in the account. Not only does the wallet software store the public and private keys, it also can generate new keys at the user's request. The wallet software can be kept on a user's digital device or can be provided by a web-based third party service. If the wallet is stored on the user's device, transactions can only be initiated from the

device the wallet is on. If a web-based wallet is used, a user can conduct transactions from anywhere as long as he can access the internet and connect to the third party service.

15. BTCs are not inherently illegal and have known legitimate uses, but based on my training and experience and information provided to me by others, they are also known to be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which BTC can be used to hide and move money anonymously. Moreover, BTC is the primary digital currency used to buy and sell illicit goods on Darknet marketplaces.

FACTS SUPPORTING PROBABLE CAUSE

A. Evidence of West's Hacking Activities

16. In connection with West's December 2015 arrest, agents recovered electronic evidence including a USB device. Through digital forensic examination, files recovered from the USB device included:

a. Falsified webpages or scam pages for U.S. companies, including Apple and Facebook. Based on my training and experience and the training and experience of the agents to whom I have spoken, these websites are typically set up as part of spam campaigns in which unsuspecting users provide their usernames and passwords to what they believe are legitimate websites.

b. Numerous AVIOS (British Airways miles) account details. These details were from accounts not belonging to West, and he had no known legitimate reason for possessing them.

c. Numerous screen shots of the Sentry MBA "hacking" software

d. Images of West

e. Compromised Personally Identifiable Information (PII) and account information of customers from financial institutions, including American Express, USAA Federal Savings Bank, Bank of America, Bank of Hawaii, JP Morgan Chase, Chase Manhattan, Black Hills Federal Credit Union, Nationsbank of Delaware, and Wells Fargo Bank. The victims are residents of Texas, Massachusetts, Kentucky, South Carolina, California, Michigan, New York, and Alabama.

17. Evidence recovered from a Samsung smart phone seized from West included:

a. One of the most frequently visited websites was LocalBitcoins.com.[2]

b. A Skype conversation log between West, utilizing the user name Trap, and an unknown subject called ÏllÏd@n †hé |3étr@yér<3 |)ö†À™•°[3] who has a Skype account name of DrugTitoo ("DT").

c. West and DT had lengthy conversations where they discussed running SentryMBA attacks against numerous companies. On 09/23/2015, West asked for DT's assistance in setting up the configuration file for a Sentry attack against a company called Just Eat. West asked DT if he/she, "wants paying for the JE config file" or if he/she wanted to join him on the campaign. On 09/23/2015, West stated he has been "hitting" Just Eat for over 3 weeks, with over 1000 results.

d. On 09/23/2015, West requested a progress report on the hacking of Just Eat and a company called Costa Coffee. DT replied, "JustEat is f******g crazy" and sent

---

2 Localbitcoins.com (LBC) is an online platform which offers advertising, messaging, BTC wallets, and escrow services for buyers and sellers of BTC. Individuals frequently use LBC to liquidate BTC undetected outside of the regulated MSB's and other financial systems.

[3] This use of symbols, numbers, and letters are typical of an online name or "handle" in the hacking community.

West a link (which is believed to be a screen capture of a Sentry MBA inquiry). West replied, "oh so you made it." DT informed West that every tenth attempt was successful. West then stated there was nothing significant inside the Just Eat accounts, but that it was useful for spamming campaigns. West added the information would assist his scam page campaigns.

e. On the same day, West asked DT if he/she wanted to sell West all the accounts or if he/she wanted to join West on a spam campaign. West also said he had not managed to capture all the account data.

18. The above indicates West compromised online accounts and then sought to monetize the stolen information through sale.

19. On 02/01/2017, UK authorities arrested West on suspicion of Fraud at the Travelodge Hotel, London Docklands E14, UK. Police searched West's hotel room and two bags and found and seized the following items of note:

a. A quantity of British Sterling cash totalling £853.15 (Equivalent to $921.40 on that date)

b. One (1) Samsung smart phone

c. Four (4) cheap mobile phones

d. One (1) HP laptop computer

20. Recovered from the laptop were thousands of user account details for U.S. companies to include: Uber, AirBNB, FitBit, NetFlix & Groupon, as well other compromised financial account information.

21. Each of the above companies were represented in West's laptop by the presence of large Microsoft Excel files. Each file contained password and logon credentials for those

companies. Each file was named by company to which the credentials applied, for example, "AirBNB.xlsx," "fitbit.xlsx," "Groupon.xlsx," "uber.xlsx," etc. Each file contained between 500-4,000 separate logon details and associated passwords. West, who was not employed by any of those companies, had no legitimate reason to have that information.

22. The UK Crown Prosecution Service was consulted in this investigation and, as a result, authorized charges of Conspiracy to Defraud against West and his child's mother. The particulars of the offense are that:

a. "Between 07/01/2015 and 12/08/2015 at within the jurisdiction of the Central Criminal Court conspired together and other persons to defraud the U.K. company Just Eat and customers of Just Eat."

23. On 03/22/2017, West was charged in the UK and made no comment. West is scheduled for trial on the 03/05/2018.

24. Other investigations continue into the compromised account information recovered from West, his other criminal activities, and money laundering.

B. <u>Evidence of West's BTC Usage</u>

25. Incident to the arrest of West on 12/08/2015, the MPS conducted a search of his residence. In the rear bedroom, hidden behind a picture frame, were a number of folded pieces of paper. The email address grantbestWest@gmail.com was written on one of the pieces of paper. Also behind the picture frame were a quantity of BTC "paper wallets." These were printed on paper and provided both the public and private keys, as well as the 12-word recovery

phrase, to access the wallet[4]. The information was also contained in a QR code[5], or quick reference code. This enables one to easily scan and store BTC into a digital device.

26. Each document had a different BTC address printed as well as the public key ("BTC address") and the private key. There was also a unique "QR" code to allow the information to be uploaded to a different software wallet.

27. The aforementioned BTC addresses are provided in a short table form below. The value of BTC can be located online. In this investigation, www.xe.com was utilized to determine BTC value.

BTC address	Source	Value on 12/08/15 in BTC	Value on 12/08/15 ($)
1CWaV71STt9vjxyLvWhkoQjaRc5SccAQCj	Listed on paper recovered from West's home address	0	$0.00
1Q3DGaCwjSbogNwXydsQR7Ggoz1VLuSZGj		0.00362198	$1.42
1MVp1CpbKS33MpgFFvbb9JyRtw2yim5wGg		2.60769811	$1,029.22
17mjrpg9VsCxzQWoamsEKNMwejD99ZQdzp		46.36638748	$18,300.22
14n346TiT8LVS539hySHxQqErfeEheavHi		77.87006182	$30,734.32
1GAPrnpTu6EHhRNqH5Xx9rhHfB5nnRkhUv		0	$0.00
18Cd1SinWDMjRRqxsgKL6Kr2LHAAXQQD6f		0	$0.00
1B8PGX6Ske7XrEjne8MFWhY9cGvihoWwP6		0	$0.00
1Q4LzTHKXxnuNGZrnzy1e1QnUuVBsJ3N3w		99.93403251	$39,442.70
1BfYnPhLuM3QYdsnufFSUHGbExpZQFpc1L		0	$0.00
Total		**226.7818**	**$89,507.88**

[4] It is common for BTC users to keep a printed copy of their keys in case the digital version of their wallet is compromised.

[5] A QR Code is an image, much like a barcode used in retail, that can be scanned by a digital device to obtain information. In this case the QR code contained BTC public and private keys.

28. Also recovered from the same location as the paper BTC wallets was a printed email from Blockchain.com. This email was addressed to grantbestWest@gmail.com. This document contained details of his online wallet account information.

29. The BTC Blockchain is an open and public distributed ledger which records each and every BTC transaction. The Blockchain records the public addresses on the sending and receiving ends, a date and timestamp, and the BTC transaction amounts. By examining the Blockchain, investigators can often successfully follow BTC transactions from one address or wallet to another. In addition, a number of websites, such as Blockchain.info or walletexplorer.com, allow one to view the Blockchain and use different analytical tools to search for data contained in the Blockchain. These websites also provide BTC wallet services.

30. Using the clustering analysis tool at walletexplorer.com, the BTC addresses 1MVp1* (abbreviated), 17mjr*(abbreviated), 1Q4Lz* (abbreviated) & 14n34* (abbreviated) are all believed to be part of the same wallet, and all of them were recovered in paper form from West's residence.

31. Wallets are a collection of BTC addresses under the administration of an individual or entity. The wallet may be managed via a software program or an online service. There are other BTC addresses that are also believed to be attributed to this wallet and, therefore, to West. A summarized table is detailed below as well as the balances on 12/08/2015. The entries in bold were recovered in paper form. BTC wallets generate a high volume of BTC addresses with which to receive change from transactions or to effect other transactions. The BTC addresses law enforcement identified came from West's possessions and these are listed in the table below in **bold font**. Because the other BTC addresses are in the same wallet, it would

be highly probable they are under West's control. Wallets are comparable to other online personal accounts (Email, bank, etc.). Items within the same wallet are under the control of the wallet owner. As the printed BTC addresses seized were in West's possession and directly attributable to him, it can be reasonably inferred that he was in control of the wallet containing the other BTC addresses. It should be noted that the other BTC addresses have a zero balance with no transactions. As controller of this wallet, West would have the ability to generate these other addresses.

Wallet address	Source	Value on 12/08/15 in BTC	Value on 08/12/15 ($)
1MVp1CpbKS33MpgFFvbb9JyRtw2yim5wGg	**Wallet 118147f16b, Wallet Explorer.com**	**2.60769811**	**$1,029.22**
1ByKigLzLK8w9GWVf8hRBXzCydpsXjANiQ		0.00000000	0.00
1DiS8SzDuXMQBx5KoXRsVE21uD2HVsbaf		0.00000000	0.00
17mjrpg9VsCxzQWoamsEKNMwejD99ZQdzp		**46.36638748**	**$18,300.22**
1JwE49YB11DtgfDprFv5FuM7GvCLMsHXyy		0.00000000	0.00
1MwosF5ARwuZmGnc5t8aJw7YCvMpaVDVxn		0.15677636	$61.88
14n346TiT8LVS539hySHxQqErfeEheavHi		**77.87006182**	**$30,734.32**
141C9fTMwtawRFvLQrEo5DmJQYQrCqaqUF		0.00000000	0.00
1AhLHY7aNnAgeHvt7CDn2ZaGpiBmoCGm9z		0.00000000	0.00
13vXjRjwZ45e8jaxNMrpVTZPjkHn6czHu7		0.00000000	0.00
1Q4LzTHKXxnuNGZrnzy1e1QnUuVBsJ3N3w		**99.93403251**	**$39,442.70**
1G7oaeRQprvjHZ65mymZHYbtXEbH2wseSV		0.00000000	0.00
1Msus2aGLHzGQzhXUPdk9JSmHvLc3iTPo2		0.00000000	0.00
15VHSxeh76ZVTtG54RCC2eEZ48TGWowb7p		0.00000000	0.00
1AnE9TGkaKvPpTN7jEAxi8gdQhSbRqsbY8		0.00000000	0.00
Total		**226.7818019**	**$89,569.76**

32. The BTC balance for all of the accounts within West's wallet totalled 226.7818019 BTC. On 12/08/2015, 226.7818019 BTC was valued at $89,569.76. On 08/25/17, 226.7818019 BTC was valued at **$986,503.11**.

C. **West's Post-Arrest BTC Movements**

33. In the United Kingdom law enforcement system, suspects are often arrested, interviewed, and released pending further investigation (i.e. review documents and digital evidence seized incident to arrest) before charges are filed, and the suspect is ordered to turn him/herself in to the police. West was released from custody on 12/08/2015, pending further investigation, after he was arrested. It is believed West re-established control of the aforementioned BTC addresses and conducted numerous transactions (as detailed below). This could have been facilitated through the use of a web-based wallet (which is provided by online vendors). With the use of the password, West would have full access and control of his funds held in the BTC addresses.

34. West was released from custody at Medway (Kent), UK at approximately 11pm on the 12/08/2015. Police had, by the time of his release, seized all electronic devices located in West's residence and on his person.

35. Transactions of note are detailed in the Appendix to this affidavit. This table lists the publicly available transactions on 12/08/2015.

36. Analysis of the transactions revealed:

- On 03/28/2015, 17mjr* sent 26.94 BTC to 1Q4Lz*
- On 12/09/2015, numerous transfers were made from BTC addresses recovered from West's residence. Namely, from 1Q4Lz*, 17mjr* & 14n34*. The transfers

were small payments of approximately 0.2 BTC. The transactions were promptly transferred back to the addresses seconds or minutes later.

Based on my training and experience, this activity is typical in money laundering where small monetary quantities are transferred to money mule bank accounts to ensure that the accounts can receive the funds. Following test payment, larger sums are subsequently transferred. In this instance, the test payments were swiftly returned. The reason for the returns is, as yet, unknown to investigators.The recipient BTC addresses were 1AzkpQJadXx55p6RnpPxg1QNPjmiFdq7Yv ("1Azkp*"), 1H3gThSiEW1gXYFMef9QbKfrrwk4yWc5na ("1H3gT*"), and 1LinRpxZmG5iFZbuk7Bi9bz2R4NiVnX42D ("1LinR*"). As shown in item #30, these recipient addressed are part of a wallet controlled by West and these transactions represent West's attempts to distribute BTC into several accounts that he owns.

37. An example is as follows:

- At 01:18:11 hours on 12/09/2015, 17mjr* sent 0.2 BTC to 1Azkp*. This transaction was confirmed at 01:24:07. Within one minute, another transaction was initiated from 1Azkp* to 17mjr* of 0.1999 BTC (0.2 BTC minus a transaction fee).
- At 01:25:01 additional small payments were sent and then received between 17mjr*, 1H3gT*, and 1LinR*.
- At 01:28:48 larger payments were then made from 14n34*, 17mjr*, and 1Q4Lz*. In total, 224.180531 BTC was transferred.

- In summary, 14n34* sent funds to 1H3gT*, and 1LinR*; 17mjr* sent funds to 1Azkp*, 1H3gT* & 1LinR*. 1Q4Lz* also sent funds to 1Azkp*, 1H3gT*, and 1LinR*.

38. The recipient BTC addresses had not been active until 12/09/2015 – the day of West's arrest. 1Azkp* first received a transaction at 01:18:11 hours. It was active until 03/21/2017. It currently has a balance of 0.15751231 BTC.

39. 1H3gT* was also inactive until 12/09/2015 when it received 0.2 BTC at 01:25:52 hours. It was active until 03/20/2017. This account has a current balance of 0.00610119 BTC.

40. 1LinR* was inactive until 12/09/2015 when it received 0.2 BTC at 01:25:01hours. It has a current balance of 0.05117026 BTC.

41. Walletexplorer.com indicated all three accounts are from the same wallet (or collection of BTC addresses), wallet address 0000059107d044d0. This is also corroborated by the transactions from the BTC addresses that were discovered in paper form as they also promptly returned funds to West's BTC address. The short time span between transfers identified in Paragraphs 38-40 indicates that the same person likely controls all of the addresses.

42. Additionally, transfers to those addresses were made following West's release from custody. Based on your affiant's training and experience, this type of activity indicates an effort by West to move his BTC from BTC addresses known to law enforcement to new addresses that were not revealed in the search of his residence.

Wallet address	Source	Value on 12/08/15 in BTC	Value on 07/04/17 (BTC)	Value on 07/04/17 ($)
1AzkpQJadXx55p6RnpPxg1QNPjmiFdq7Yv	Wallet ID 304ecb8691a8737d, Wallet Explorer.	0	0.15751231	359.13
1LinRpxZmG5iFZbuk7Bi9bz2R4NiVnX42D		0	0.05117026	116.67
1Bb2S8eXisVzRCrxW7mBDc8BQrZCL8VAu8		0	0.00997385	22.74
1MdRzBsHX8i1jzi1E58Y5btBn6pvxG8amV		0	0.00835064	19.04
1BJRnTFoq1kR2ZtWmazzdwcEthn2VaET4		0	0.00662501	11.21
1H3gThSiEW1gXYFMef9QbKfrrwk4yWc5na		0	0.00610119	13.91
Total			**0.23973326**	**542.70**

43. The activity of the BTC addresses in the wallet, namely 1Azkp*, 1H3gT* & 1LinR* revealed that up until 03/10/2017, significant quantities of BTC were transferred to wallet address 0000059107d044d0. That wallet address is attributable to Poloniex, as explained below. From 03/08/2016 to 03/10/2017, 286 BTC were sent to this wallet. Investigations continue as to the individual(s) associated with this wallet. It is believed there is a balance of 154.301 BTC held by the wallet, and that the BTC in the wallet belongs to West.

44. Online WalletExplorer.com inquiries revealed wallet address 0000059107d044d0 is managed by the Delaware-based BTC exchange, Poloniex. Further investigation has revealed that Poloniex maintains a wallet under the control of West.

45. It is believed that West continues to use BTC to conduct financial transactions. He continues to fund his lifestyle with no legitimate means of employment or earnings. Credit

agency and UK National Tax Office inquiries revealed West does not possess a traditional bank account at that time. Investigators determined West only recently opened a bank account to receive State benefits (the equivalent of Welfare benefits in the United States). This account was opened earlier this year, does not receive any salary deposits, and has a balance of £300 (~$404 USD). He has continued his criminal enterprise on the dark web, which based on my experience and training, necessitates the use of digital or cryptocurrency such as BTC. West continues to generate significant income and his arrest has not deterred him.

46. On 7/6/17, Poloniex blocked West's access to his wallet due to suspicious activity. Since that time West has made several attempts to access this wallet and made several complaints to Poloniex in reference to the block. These attempts to access the wallet indicate that (1) West still has significant BTC holdings in the Poloniex account; and (2) that West is indeed the owner of that account.

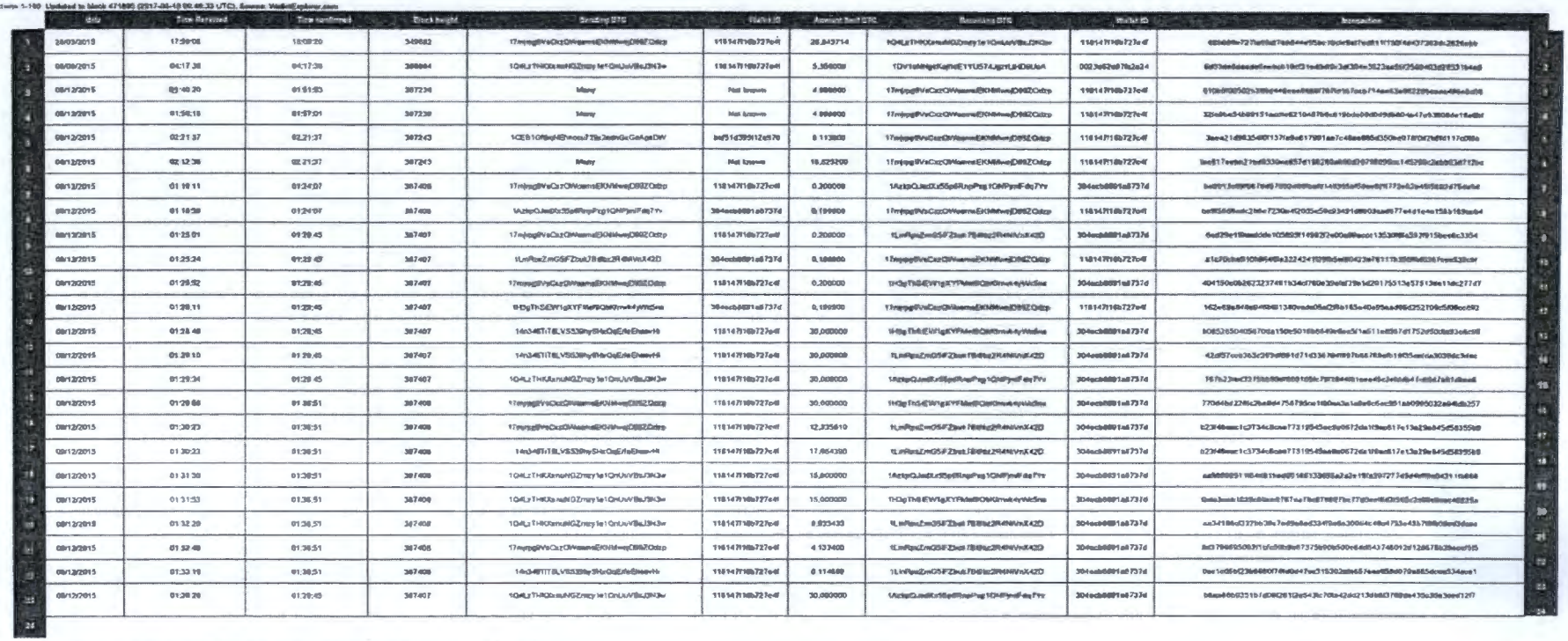
47. It is respectfully requested that this Court issue and order sealing, until further order of the Court, all papers submitted in support of this application, including the application and seizure warrant. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Special Agent Scott M. McDerby

Subscribed and sworn to before me on September 28, 2017

HON. CHRISTOPHER J. BURKE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF DELAWARE



Time Received — The time the transaction was received by the network, this may not be in sequence due to the nature of the BitCoin network
Time Confirmed — This is the time the "miners" have produced the block of transactions and have confirmed that the transaction details are correct. This then means that the transaction is committed to the BlockChain
Block Height — The number of the Block in which the transaction appears on the BlockChain